

REMARKS

The present Amendment amends claims 1-4, 6, 13-16, 19, 25-28, 31 and 37, leaves claims 5, 6, 17, 18, 29 and 30 unchanged and cancels claims 8, 20 and 32. Therefore, the present application has pending claims 1-7, 13-19, 25-31 and 37.

Claims 1-8 stand rejected under 35 USC §101 being that the Examiner alleges that the claimed invention is directed to non-statutory subject matter particularly a computer program. As indicated above, claim 8 was canceled. Therefore, this rejection with respect to claim 8 is rendered moot. With respect to the rejection of the remaining claims 1-7, it should be noted that claims 1-7 are now directed to a method performed by a computer. Therefore, this rejection is overcome and should be withdrawn.

Claims 1-8, 13-20, 25-32 and 37 stand rejected under 35 USC §112, first paragraph as allegedly being based on a disclosure which is not enabling and claims 1-8, 13-20, 25-32 and 37 stand rejected under 35 USC §112, as being incomplete for omitting essential elements, such omission amounting to a gap between the elements. As indicated above, claims 8, 20 and 32 were canceled. Therefore, these rejection with respect to claims 8, 20 and 32 are rendered moot. These rejections with respect to the remaining claims 1-7, 13-19, 25-31 and 37 are traversed for the following reasons. Applicants submit that the features of the present invention as now more clearly recited in claims 1-7, 13-19, 25-31 and 37 fully complies with the requirements of 35 USC §112, and as such the subject matter recited in the claims are in fact based on a disclosure that is enabling and the subject matter as recited in the claims is

complete being that the essential elements of the invention are recited in the claims. Therefore, reconsideration and withdraw of these rejections is respectfully requested.

It should be noted that the claims as amended are based on a disclosure that is enabling being that the claims now recite a dividing plaintext operation or step which corresponds to the flowchart and the corresponding description of Fig. 2, a generating first and second random number blocks operation or step which corresponds to the flowchart and corresponding description of Fig. 3 and performing encryption operations and concatenating the series of ciphertext blocks operations or steps which correspond to the flowcharts and corresponding description of Fig. 4. Therefore, the claims as now written are in fact based on an enabling disclosure.

In the Office Action the Examiner alleges that essential elements are omitted from the claims and identifies such essential elements as two computers connected over a network, padding, a pseudo-random sequence, a counter, a series of ciphertext blocks, and concatenates the series of ciphertext blocks one after another sequentially. Applicants submit that the elements identified by the Examiner are not essential elements of the invention and as such need not be recited in the claims. However, the claims were amended to recite that the method is performed by a computer, that first and second random number blocks are generated, that a series of ciphertext blocks are produced and that such series of ciphertext blocks are concatenated.

Therefore, based on the above, Applicants respectfully request the Examiner to reconsider and withdraw the 35 USC §112, first and second paragraphs rejections.

Claims 1-8, 13-20, 25-32 and 37 stand rejected under 35 USC §102(e) as being anticipated by Shukla (U.S. Patent No. 6,345,101). As indicated above, claims 8, 20 and 32 were canceled. Therefore, this rejection with respect to claims 8, 20 and 32 is rendered moot. This rejection with respect to the remaining claims 1-7, 13-19, 25-31 and 37 is traversed for the following reasons. Applicants submit that the features of the present invention as now more clearly recited in claims 1-7, 13-19, 25-31 and 37 are not taught or suggested by Shukla whether taken individually or in combination with any of the other references of record. Therefore, Applicants respectfully request the Examiner to reconsider and withdraw this rejection.

Amendments were made to the claims so as to more clearly describe features of the present invention. Particularly, amendments were made to the claims in order to more clearly describe that the present invention is directed to a symmetric key encryption method, apparatus, computer program and program product as recited, for example, in independent claims 1, 13, 25 and 37. The present invention as recited in said claims provides:

(1) a first random number block and a second random number block are applied to the same plaintext block i throughout the encryption operation related to the plaintext block i , and

(2) an intermediate result of an encryption operation performed on the plaintext block i is used, as a feedback value, for another encryption operation performed on the plaintext block i that follows.

The above described features of the present invention now more clearly recited in the claims are not taught or suggested by any of the references of record particularly Shukla whether taken individually or in combination with each other.

Shukla discloses a cryptographic method that belongs to a symmetric-key encryption method and generates a random number block corresponding to a plaintext block. However, there is no teaching or suggestion in Shukla of the encryption operation of the present invention as recited in the claims.

Shukla's encryption operation consists of a series of rounds. Each of the plaintext blocks goes through one series of the rounds. One of the rounds consists of an XOR1 operation, a shuffle operation and an XOR2 operation, and these operations are executed in this order, as shown on Fig. 3 thereof. The XOR1 operation performs an XOR operation on a plaintext block D and a random number block S. The shuffle operation shuffles the bits of the result (D1) of the XOR1 operation in accordance with each bit value of a private key K. The XOR2 operation performs an XOR operation among the bit strings of the result (D2) of the shuffle operation.

The encryption operation as recited in the claims includes first, second and third operations which are quite different from the teachings of Shukla.

For example, the second operation step in the present invention as recited in the claims uses the second random number block, whereas Shukla's second operation (the shuffle operation) does not use a random number block as in the present invention.

Further, for example, the third operation step in the present invention as recited in the claims performed on the plaintext block i uses, as a feedback

value, a result of the first operation step that has been performed on the plaintext block $i-1$, whereas Shukla's round operations on a plaintext block D do not use a result of the operations performed on another plaintext block as in the present invention.

Thus, Shukla fails to teach or suggest performing encryption operations for producing ciphertext blocks each corresponding to each of the plurality of plaintext blocks and concatenating the series of the ciphertext blocks one after another sequentially to output the series as the ciphertext as recited in the claims.

Further, Shukla fails to teach or suggest that one of the encryption operations for producing the ciphertext block i corresponding to the plaintext i ($2 \leq i \leq$ a number of plaintext blocks) comprises a first operation step for performing an arithmetic computation on the plaintext block i and the first random number block corresponding to the plaintext block i , a second operation step for performing an arithmetic operation on a result of the first operation step performed on the plaintext block i and the second random number block corresponding to the plaintext block i , and a third operation step for performing an arithmetic computation on a result of the second operation step performed on the plaintext block i and a result of the first operation step performed on the plaintext block $i-1$, to produce the ciphertext block i as recited in the claims.

Still further, Shukla fails to teach or suggest that either the first random number or the second random number is generated in complete isolation from any one of the plurality of plaintext blocks or the result of the second operation step as recited in the claims.

Therefore, Shukla fails to teach or suggest the features of the present invention as now more clearly recited in the claim's. Accordingly, reconsideration and withdrawal of the 35 USC §102(e) rejection of claims 1-7, 13-19, 25-31 and 37 is respectfully requested.

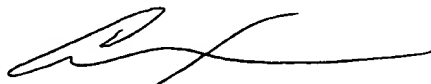
The remaining references of record have been studied. Applicants submit that they do not supply any of the deficiencies noted above with respect to the references utilized in the rejection of claims 1-8, 13-20, 25-32 and 37.

In view of the foregoing amendments and remarks, applicants submit that claims 1-7, 13-19, 25-31 and 37 are in condition for allowance. Accordingly, early allowance of claims 1-7, 13-19, 25-31 and 37 is respectfully requested.

To the extent necessary, the applicants petition for an extension of time under 37 CFR 1.136. Please charge any shortage in fees due in connection with the filing of this paper, including extension of time fees, or credit any overpayment of fees, to the deposit account of MATTINGLY, STANGER, MALUR & BRUNDIDGE, P.C., Deposit Account No. 50-1417 (520.39632X00).

Respectfully submitted,

MATTINGLY, STANGER, MALUR & BRUNDIDGE, P.C.



Carl I. Brundidge
Registration No. 29,621

CIB/jdc
(703) 684-1120